

Investigation into igg-games & gamestorrent

Date of publication - November 26th, 2018

Overview

The purpose of this document is to summarize information found online that reveals the identity of the individuals that operate the gaming piracy websites "igg-games.com" (<http://igg-games.com/>) and "gamestorrent.co" (<http://gamestorrent.co/>) which profit from the distribution of illegal copies of video games via advertisements (pop-up ads, etc). At the time of publication, they are ranked 1,305 and 5,958 globally by [Alexa.com](https://www.alexa.com/).

Establishing a Commonly Used Username

We must first identify a username used by the website owners on other sites or forums. As both websites use the content management system [WordPress](#); we decided to look there.

The tool we are using to accomplish this is [WPScan](#). Here are the full scan results for both sites:

- igg-games.com | <https://pastebin.com/FQHwRjQg>
- gamestorrent.co | <https://pastebin.com/iUnnSjBk>

We uncover the same WordPress username for both sites: vietphap123

```
[i] User(s) Identified:
[+] vietphap123
| Detected By: Author Posts - Author Pattern (Passive Detection)
| Confirmed By:
|   Wp Json Api (Aggressive Detection)
|     - http://igg-games.com/wp-json/wp/v2/users/
|   Author Id Brute Forcing - Author Pattern (Aggressive Detection)
|   Login Error Messages (Aggressive Detection)
```

We have located the administrator account creating new posts on each website. As you can see here:

- <http://igg-games.com/author/vietphap123> | <http://archive.is/k17LE>
- <http://gamestorrent.co/author/vietphap123> | <http://archive.is/2G4Ti>

Online Profiles

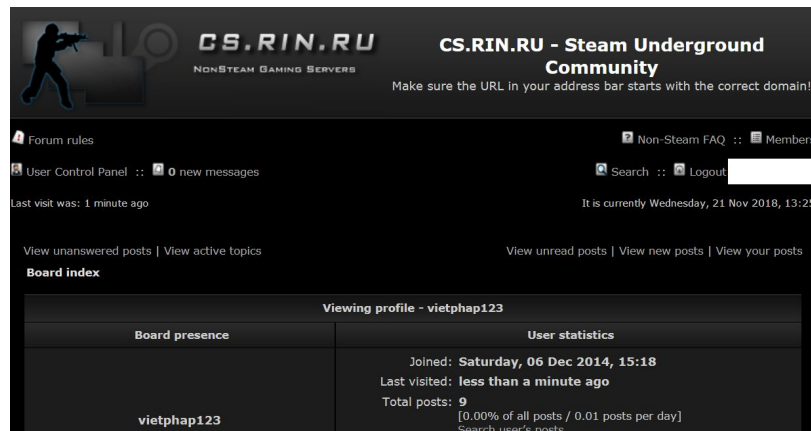
Searching on Google reveals many hits for **vietphap123**:

[https://www.google.com/search?q=\"vietphap123\"](https://www.google.com/search?q=\)

Here are the important ones which we will mention:

1. User vietphap123 on the OVH forums wanting to purchase a VPS (writes: “I think i will buy VPS at Online.net, bye”):
<https://forum.ovh.co.uk/showthread.php/9060-I-can-t-pay-for-VPS> | <http://archive.is/gIAHH>
2. “IGGGAMER” WordPress site: <https://igggamer.wordpress.com/author/vietphap123/> | <http://archive.is/lyhu4>
3. Blogger.com site (Vietnamese): <http://vietphap123.blogspot.com/> | <http://archive.is/4TsM4>
4. Private Tracker trading forum (private trackers are a prime source for illegal copies of copyrighted content):
<https://www.invitescene.com/profile/7571-vietphap123/content/> | <http://archive.is/fVw2l>
5. vietphap123 commenting on a GoDaddy coupon (site is in Vietnamese):
<https://canhme.com/godaddy-coupon/gd-coupon-thang-10-2013/> | <http://archive.is/G4uNQ>
6. The igg-games.com Disqus account (used to manage comments on the site) is @vietphap123: <https://disqus.com/by/vietphap123/> | <http://archive.is/mCHYR>
7. vietphap123 posting a speedtest result on mmo4me.com (Vietnamese site):
<https://mmo4me.com/threads/mang-cuc-cham-ngay-ca-trong-nuoc.147482/#post-3029190> | <http://archive.is/BCgks>
8. vietphap123 on voz.vn (Vietnamese site yet again) with “gamestorrent.co” in their profile signature: <https://forums.voz.vn/member.php?u=486192> | <http://archive.is/QXsqv>
9. Google Plus user vietphap vo with an “IGG” profile picture posting facebook hyperlinks: <https://plus.google.com/110797677756935902362/posts/WSrVqARTfdG> | <http://archive.is/cn6BK>
10. YouTube profile: <https://www.youtube.com/user/vietphap123> | <http://archive.is/jj78c>
11. Facebook profile (which is deleted or has access restricted; lists two cities in Vietnam): <http://archive.fo/gf1Aa> | <https://www.facebook.com/vietphap123>
12. Steam profile (take note of the “phap” group with two members):
<https://steamcommunity.com/profiles/76561198057968528> | <http://archive.is/Nmu3l> (upon further research the other group member is named “Vietnhatvo” and their has their location as Viet Nam):
<https://steamcommunity.com/profiles/76561198065892744> | <http://archive.is/9HA9T>
13. Vidinterest account and their name as Vo Viet Phap (a real name?):
<https://vidinterest.tv/vietphap123> | <http://archive.is/n8lkD>
14. Twitter profile and their name as vo viet phap (mentions igg-games.com):
<https://twitter.com/installguidegam> | <http://archive.is/ahhPv>

15. Imgur account that is 4+ years old: <https://imgur.com/user/vietphap123/submitted> | <http://archive.is/DxgVu>
16. Photobucket: <http://s329.photobucket.com/user/vietphap123/profile/>
17. Another WordPress site that looks similar to igg-games.com: <http://cheapserver.info/author/vietphap123> | <http://archive.fo/mjYUv>
18. CS.RIN.RU account (requires to be signed in with an account to view profiles): <https://cs.rin.ru/forum/memberlist.php?mode=viewprofile&u=544112>



With the information above, we can conclude that the individuals who operate “igg-games.com” and “gamestorrent.co” are from **Vietnam** and reuse **vietphap123** as their username on various websites. Also, one of the individual’s real name is possibly **Vo Viet Phap**.

Domain & DNS History

Let’s take a look at the WHOIS history for igg-games.com:

<https://whois.easycounter.com/igg-games.com>

Investigating the matbao.net entry at the very bottom, we get an address, phone number and again the name **Vo Viet Phap**: <https://pastebin.com/E67XpF9M>

Name: Ong Vo Viet Phap

Address: 62 An Diem, phuong 10, quan 5, Ho Chi Minh 70000 Vietnam

Phone: +84.986918917

Email: vietphap123@gmail.com

Now, let’s see if we can find where the website for igg-games.com is most likely hosted:

<https://securitytrails.com/domain/igg-games.com/history/a> | <http://archive.is/FWat2>

The most recent result that is not Cloudflare is **Online S.A.S. (or Online.net)**. Recall the post from vietphap123 on the OVH forums: “I think i will buy VPS at Online.net, bye”

<https://forum.ovh.co.uk/showthread.php/9060-I-can-t-pay-for-VPS> | <http://archive.is/gIAHH>

Using the login **vietphap123** at the [Online.net login recovery](#) yields the same phone number and email address we found from past WHOIS entries:



English ▾ Subscribe Sign in
Order ▾ API Support Webmail ↗

Lost password

Please select a contact address where you want to send password recovery information

Associated contact information:

Contacts :
☐ viet*****@*mail.com *
☐ +84.9*****17 *
To ensure your privacy, only a portion of your email is displayed

Confirms they are using Online.net servers for something.

Compromised Accounts

We decided to look in leaked databases for a password linked to the username **vietphap123**. The alias is reused everywhere, so most likely the password is too.

Our suspicion was confirmed true, and many of the accounts at various sites are accessible using vietphap123 / vietphap123@gmail.com and the password we found. Some examples:

vidinterest account

vidinterest

Profile
Update your personal information

Settings

- Profile
- Password
- Verification
- Email Notification

Personal Information

Name: Vo Viet Middle Name: Phap

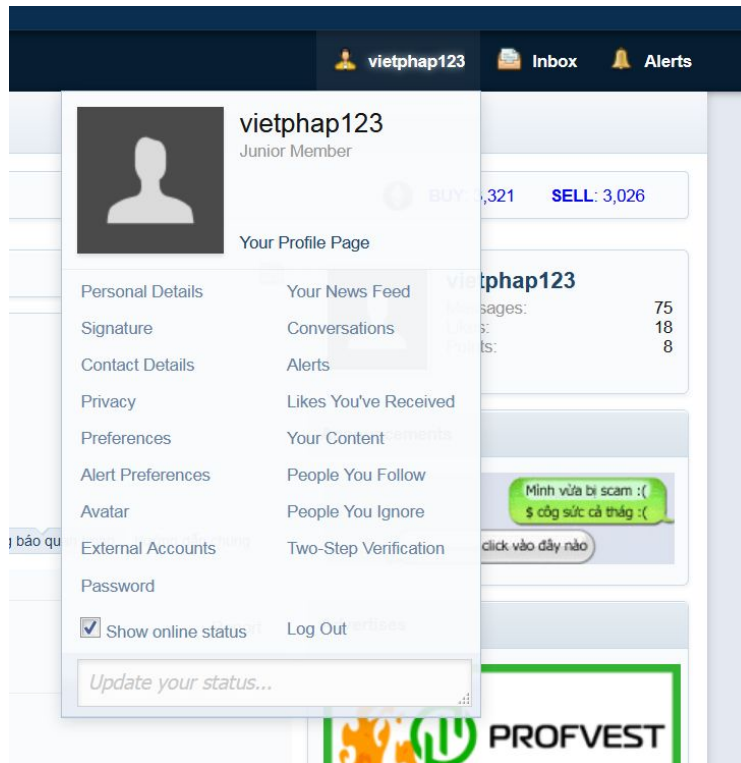
Gender *: ☒ Male ☐ Female

Username *: vietphap123 Email *: vietphap123@gmail.com

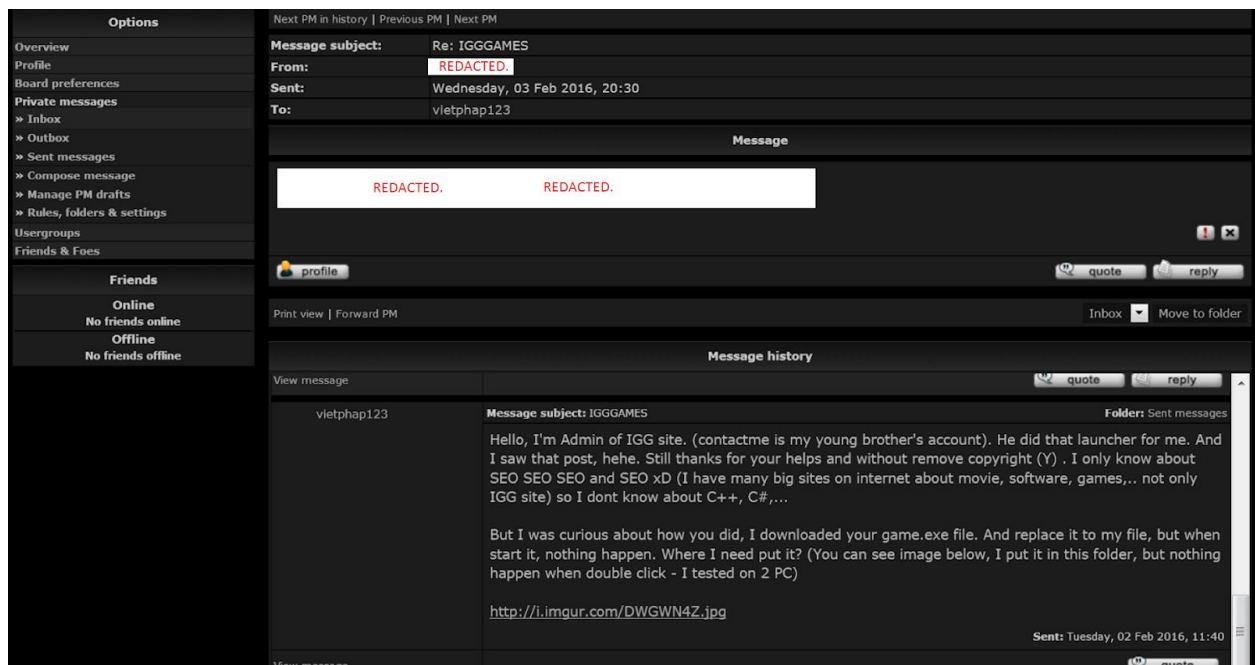
Country: -- Select Country -- City Name: Nha Trang

Website: http://

mmo4me.com account



CS.RIN.RU account - claims two brothers own and run the sites.



filehoster account “UptoBox”

My account

Free member

Hello vietphap123

Number of points UTB : **103.80275** *1 Uptobox point = 1000 downloads on Uptobox or 1000 views on Uptostream. [Convert my points](#)

My affiliate link:

My referrals: 746

Token:

You have a voucher code ? [Click here](#)

Configuration

Security lock **OFF** [Enable](#)

Direct Download **OFF** [Enable](#) ★ You must be premium to access this feature

Secure download (SSL) **OFF** [Enable](#)

Direct download on your NAS (Download Station)

My informations

Email

Dumping the Imgur Account

Most of the accounts we can login to on various websites do not provide any additional or incriminating evidence. But then we hit the motherload.

Using the same credentials, we logged into the vietphap123 imgur account (<https://imgur.com/user/vietphap123> | <http://archive.is/tjVd1>) and found it contained more than 100 unlisted images that confirm the individuals who own and operate “igg-games.com” and “gamestorrent.co” are two brothers from Vietnam: **Vo Tan Phap** and **Vo Viet Phap**.

We’ve made these images public. You can view them here: <https://bit.ly/2PWqbdS>

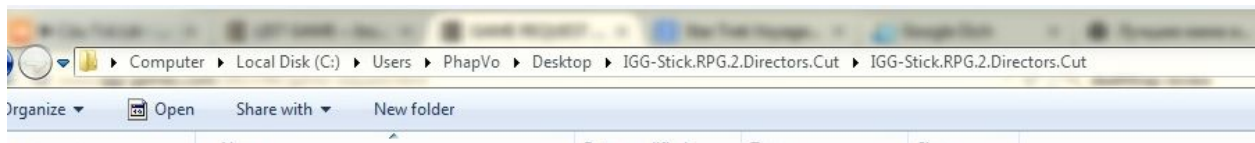
All the images from the account have been dumped and are available for download below:

Anonfiles: <https://bit.ly/2Twp4j0>

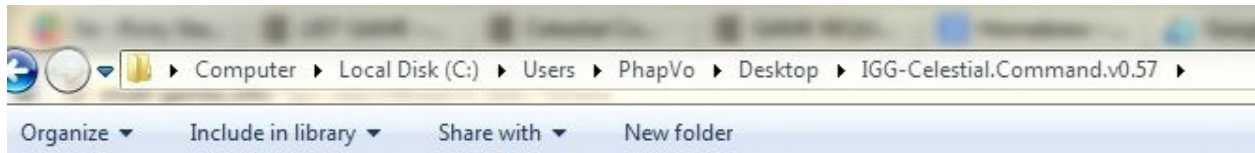
Analyzing the Evidence

There is an enormous amount of evidence provided by the images obtained from the imgur account. We are going to analyze the most important ones in this section.

In images **3 - 3Wogp5V.jpg** and **4 - oC6X667.jpg** we can see the username of the computer in the Windows directory bar: **PhapVo**. This is related closely to the name we found earlier (Vo Viet Phap) from past WHOIS information and on various online accounts:



Taken from 3 - 3Wogp5V.jpg



Taken from 4 - oC6X667.jpg

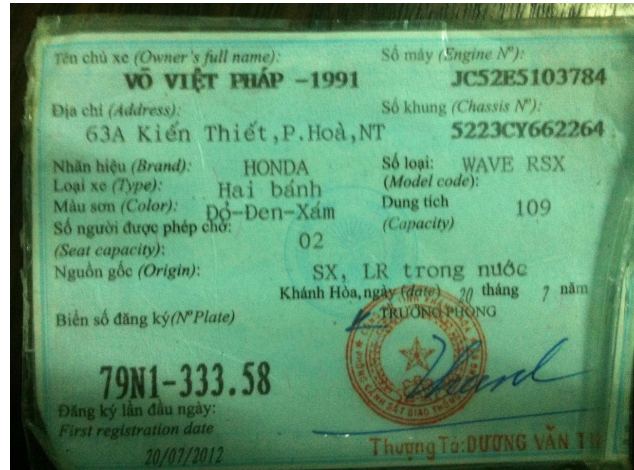
In image **18 - ubD8dHl.jpg** we have a bank deposit slip from Vietcombank. Two names are listed: **Vo Tan Phat** and **Vo Viet Phap**. The address listed for Vo Viet Phap matches the one we found from past WHOIS information for igg-games.com: **62 An Diem, phuong 10, quan 5, Ho Chi Minh**.

The details also mention this is for a virtual private server (VPS) -- **Details: “Tien VPS”**.

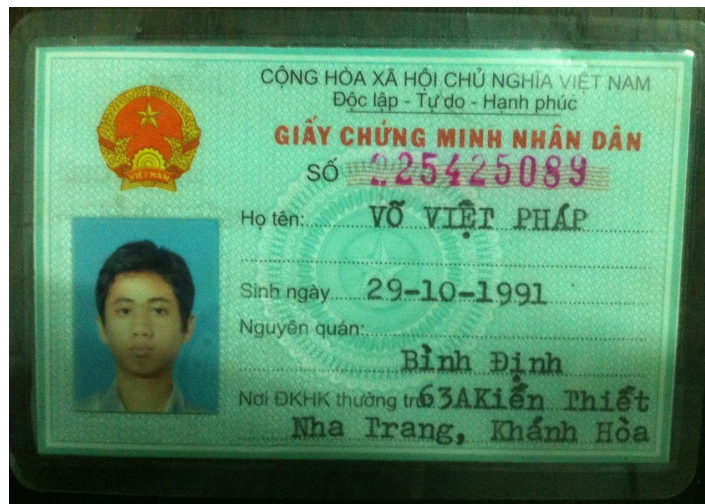
Ngân hàng TMCP Ngoại Thương Việt Nam Chi nhánh Quận 5 Địa chỉ: 2D-2E Lý Thường Kiệt, P.12 Quận 5, TP. Hồ Chí Minh MÃ VAT: 0100112437041		CHỨNG TỪ G GIẤY NỘP TIỀN Ngày (Date): 30/3/18 Số HD - Invoice No: 30031
ĐỀ NGHỊ GHI CỐ TÀI KHOẢN (Please Credit account):		
SỐ TK (A/C No.)	0721.005 101 789	
TÊN TK (A/c name):	VO TAN PHAT.	
ĐỊA CHỈ (Address):		
NGÂN HÀNG (With Bank)	VIETCOMBANK. KỶ HỒNG.	
NGƯỜI NỘP TIỀN (Depositor)		
Họ & tên (Full name):	VO VIET PHAP	
Địa chỉ (Address):	62 AN DIEM P.10, Q.5, HCM	
NỘI DUNG NỘP (Details):	TIỀN VPS	

Taken from 18 - ubD8dHl.jpg

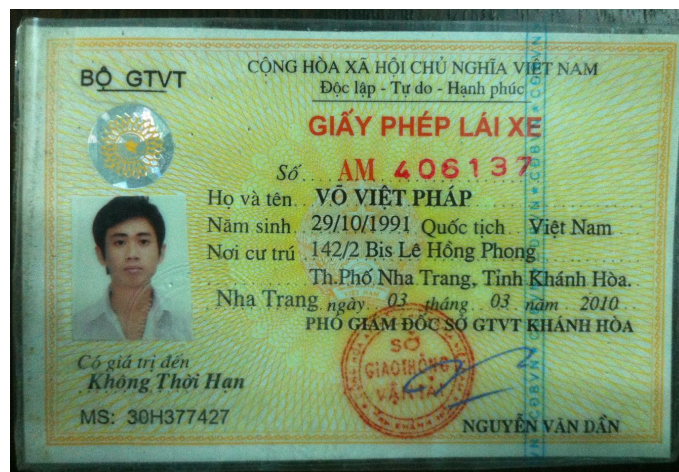
In the following images **42 - 9RLjbZj.jpg**, **43 - yZdaDUa.jpg**, and **44 - fEuZ7ve.jpg** we have identification cards for Vo Viet Phap:



Taken from 42 - 9RLjbZj.jpg



Taken from 43 - yZdaDUa.jpg



Taken from 44 - fEuZ7ve.jpg

In image **28 - 2KFmlQf.jpg** we have a PayPal user named **Viet Phap Vo** and a transaction to GoDaddy.com LLC. He is most likely paying for a domain (that is also their current registrar for both websites).

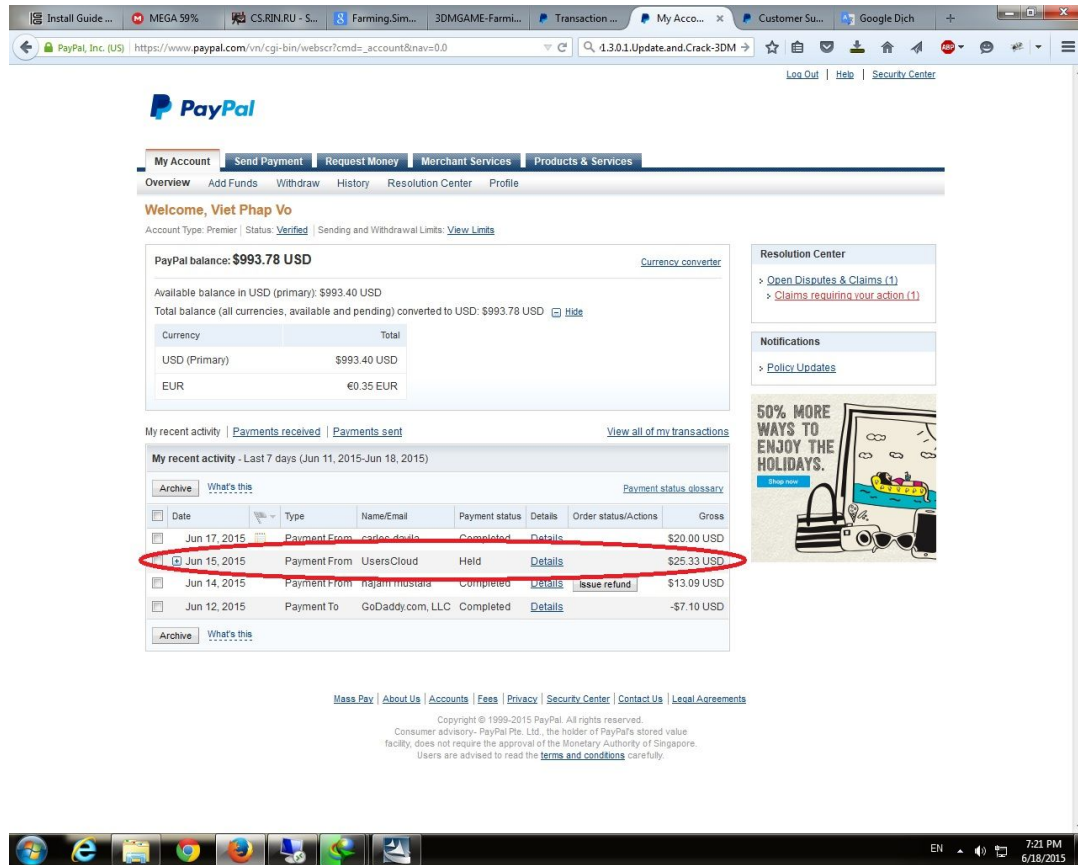


Image 28 - 2KFmlQf.jpg

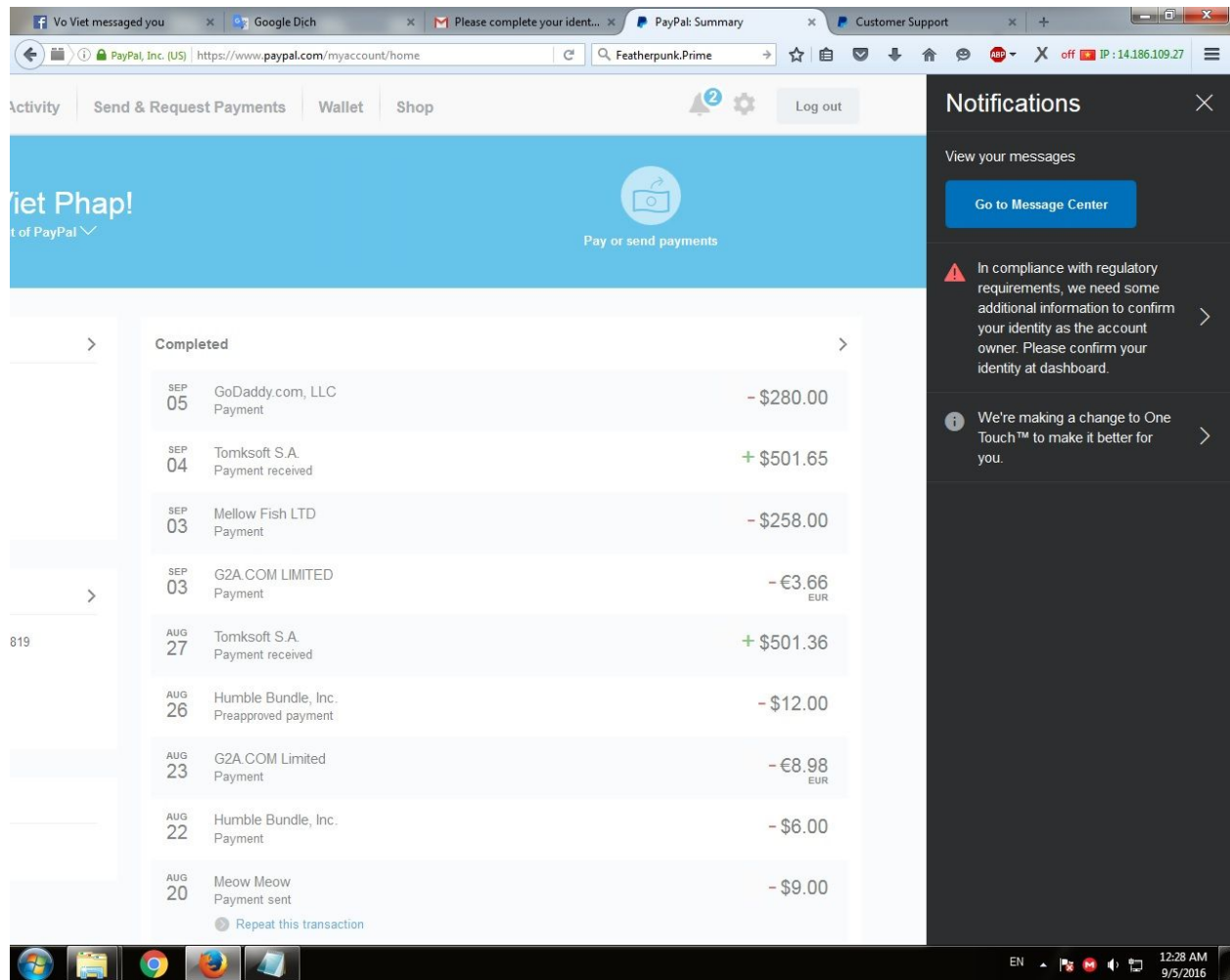
In image **74 - DuTKpMz.jpg (see below)** we have again the Paypal user Viet Phap listed, payments to GoDaddy, payments to [G2A](#) and [Humble Bundle](#) (to buy games to distribute via their website most likely) and payments received from Tomksoft S.A. **There is also a Facebook tab open that reads: Vo Viet messaged you.**

Tomksoft S.A owns [popads.net](#) which is an ad network used for generating revenue.

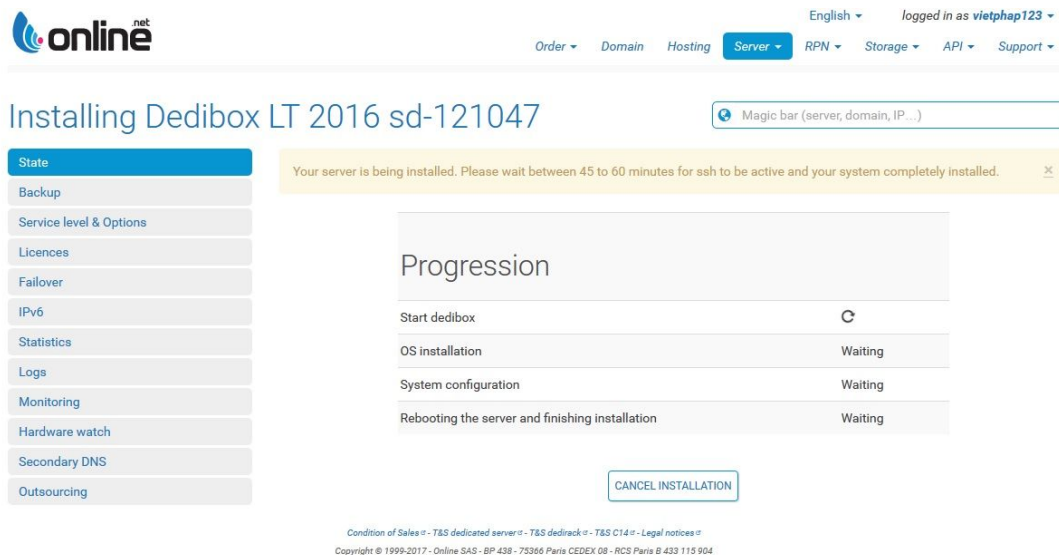
“WHEREAS, Tomksoft S.A. (Tomksoft) is a joint stock company located and registered in Costa Rica and is engaged in the business of providing Pop-under advertising through Popads.net. Popads.net is owned and operated by Tomksoft S.A.”

<https://www.popads.net/terms-of-service.html>

Image 74 - DuTKpMz.jpg



In image **103 - UPZ38qm.jpg** we see the user vietphap123 logged into their Online.net account (top left-hand corner) and installing a server:



In image **60 - nMbpq9d.jpg** we can again see the user vietphap123 logged into Online.net and a list of servers and IP addresses:

Server list

Server list in DC2

Id	Offer	IP	Reverse	Action
✓ 55016	Dedibox Classic 2015 (sd-55016)	62.210.131.67	62-210-131-67.rev.poneytelecom.eu.	Manage
✓ 79615	Dedibox XC SSD (sd-79615)	62.210.105.89	62-210-105-89.rev.poneytelecom.eu.	Manage
✗ 79963	Dedibox XC SSD (sd-79963)	Server locked (Maintenance)		

ORDER

Server list in DC3

Id	Offer	IP	Reverse	Action
✗ 49033	Dedibox Classic 2015 (vietphap6)	62.210.209.178	62-210-209-178.rev.poneytelecom.eu.	Manage

ORDER

In image **79 - tuMltpF.jpg** we have a Steam receipt with the username vietphap123 listed:

Thank you for your Steam purchase!

Hello vietphap123

Thank you for your recent transaction on Steam. The items below have been added to your Steam Library.

If you are new to Steam, you can get the free Steam application [here](#).

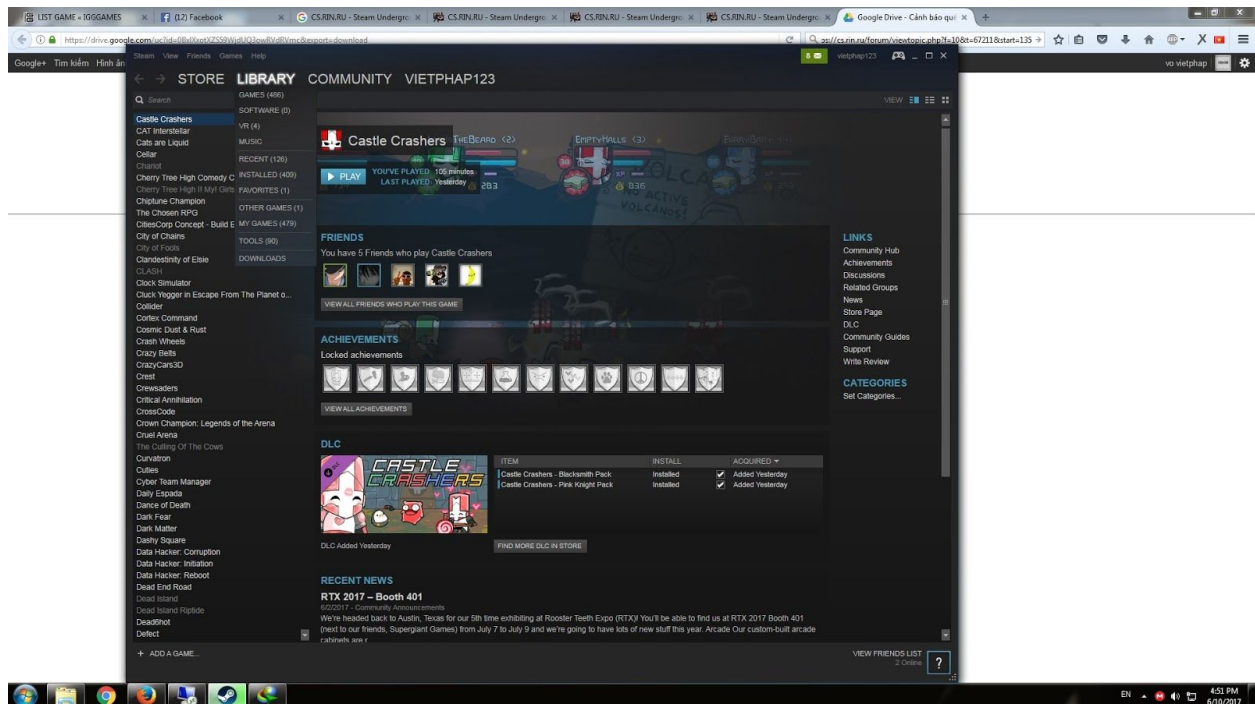
Dungeons & Robots	\$8.99
Total:	\$8.99

Account name: vietphap123
Invoice: 940514869255863555
Date issued: 3 Oct, 2016 @ 10:02am PDT
Payment method: PayPal

This email message will serve as your receipt. You can also [view your Purchase History](#) at any time.

Refunds and/or returns may be granted for many products on Steam. Learn more

In image **95 - GPW3rxi.jpg** we can see them logged into their Steam account: [vietphap123](#):



These are all the images we want to touch on. There are even more in the complete dump you can look at (such as screenshots of the old IGGGAMES kickasstorrent profile & messages with a user and a moderator, private tracker usernames, browsing private tracker trading forums and more).

Again, you may download a complete set of the images from the imgur account dump at:

Anonfiles: <https://bit.ly/2Twp4j0>

PayPal Account

We discovered a test page which contains their paypal account email address

"iggcontact123@gmail.com": <http://igg-games.com/test.html> | <http://archive.is/M2qBe>

Final Thoughts

Remember folks, don't be like these imbeciles and reuse your username, email and password all over the internet -- especially when you operate a high-profile website focused on piracy.

Who knows, maybe bringing this information to light will get a formal investigation started. Trying to remain anonymous seems to be at the bottom of their priority list.